PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-236325
(43)Date of publication of application : 31.08.2001

(51)Int.Cl. G06F 15/00
G06F 1/00
H04L 9/32

(21)Application number : 2000-045634
(22)Date of filing : 23.02.2000

(71)Applicant : MERITTSU:KK
(72)Inventor : KOREYASU TOSHIYUKI

(54) INDIVIDUAL IDENTIFICATION SYSTEM AND ITS USING METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a means for implementing a function of identifying a person who tries to operate an electronic system without any error at low cost surely and easily for the operator.
SOLUTION: The individual identification and various usages of the individual identification system are provided. The individual identification system includes as elements (1) a small-sized terminal 1 which has an infrared communicating mechanism (a) sending the individual identification information and (2) an individual identification terminal 2 having an infrared communicating mechanism (b) which can exchange the individual identification information through the infrared communicating mechanism (a).

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1]** the sized terminal 1 which has the infrared-ray-communication mechanism a which sends personal identification information -- and, ** An individual identification system which identifies an individual in this individual identification terminal 2 according to the contents of the aforementioned personal information including the individual identification terminal 2 which has the infrared-ray-communication mechanism b which can exchange the information about personal identification information through the infrared-ray-communication mechanism a as an element.
[Claim 2]Make personal identification information send from the infrared-ray-communication mechanism a, and the infrared-ray-communication mechanism b receives this personal identification information, and a case where this personal identification information is considered as conformity by collation in the individual identification terminal 2 -- the individual identification terminal 2 -- the person himself/herself -- an identification system use method according to claim 1 of identifying an individual by carrying out a reaction at the time of discernment affirmation.
[Claim 3]Dispatch of personal identification information in the infrared-ray-communication mechanism a is intermittent dispatch, and when this personal identification information sent intermittently is made incongruent by collation in the ** individual identification terminal 2, and/or, a time of it having become impossible for the ** individual identification terminal 2 to receive this personal identification information sent intermittently -- the individual identification terminal 2 -- the person himself/herself -- an identification system use method according to claim 2 of identifying an individual by carrying out a reaction at the time of discernment denial.
[Claim 4]An identification system use method according to claim 2 or 3 of random data being contained in personal identification information, including collation of this random data in an individual discernment act, and identifying an individual.
[Claim 5]An identification system use method according to claim 4 that random data is one sort or two sorts or more of random data chosen from a group which consists of pseudorandom numbers obtained by an output value and a pseudorandom-numbers generation program of a one-time password and a one-way hash function.
[Claim 6]An identification system use method of either of claims 2-5 which information enciphered by personal identification information is included, compares this information enciphered, and identifies an individual given in a claim.
[Claim 7]When a response request message is made to send from the infrared-ray-communication mechanism b and the infrared-ray-communication mechanism a receives this response request message, a case where made a response message transmit towards the individual identification terminal 2, and this response message is considered as conformity in the individual identification terminal 2 from the sized terminal 1 -- the individual identification terminal 2 -- the person himself/herself -- an identification system use method according to claim 1 of identifying an individual by carrying out a reaction at the time of discernment affirmation.
[Claim 8]Only when the individual identification terminal 2 is identifying an individual, to this

individual identification terminal 2. A specific response request message is made to send to the sized terminal 1 of a discrimination object, This sends a response message for the sized terminal 1 only to a specific response request message from this individual identification terminal 2, When the individual identification terminal 2 is changed into a state which can respond only to a response message from this sized terminal 1 and the individual identification terminal 2 furthermore is not identifying an individual,An identification system use method according to claim 7 which makes a response request message to the unspecified sized terminal 1 send to the individual identification terminal 2, and changes the sized terminal 1 into a state which can respond only to a this object unspecified response request message.

[Claim 9]An identification system use method according to claim 7 or 8 of random data being contained in a response request message and/or a response message, including collation of this random data in an individual discernment act, and identifying an individual.

[Claim 10]An identification system use method according to claim 9 that random data is one sort or two sorts or more of random data chosen from a group which consists of pseudorandom numbers obtained by an output value and a pseudorandom-numbers generation program of a one-time password and a one-way hash function.

[Claim 11]An identification system use method of either of claim 9 or 10 which information enciphered by a response request message and/or response message is included, compares this information enciphered, and identifies an individual given in a claim.

[Claim 12]** Dispatch of a response request message is intermittent dispatch, and/when a response message which receives that it can come was made incongruent in the individual identification terminal 2. or ** -- a time of it having become impossible for the individual identification terminal 2 to receive a response message over this -- the individual identification terminal 2 -- the person himself/herself -- an identification system use method of either of claims 7-11 which identifies an individual by carrying out a reaction at the time of discernment denial given in a claim.

[Claim 13]Information which is different for every response request message in a part of response request message intermittently sent from the individual identification terminal 2 is included, To and a response message sent from the sized terminal 1 to each response request message. the aforementioned information -- or the double sign of the enciphered aforementioned information being carried out, and, when information which enciphered information which processed this information is included and the individual identification terminal 2 receives this response message, case it carries out comparative collation to this double sign information and information included in the aforementioned response request message and both information is substantially the same -- the individual identification terminal 2 -- the person himself/herself -- an identification system use method of either of claims 7-11 which performs a reaction at the time of discernment affirmation given in a claim.

[Claim 14]The sized terminal 1 and the individual identification terminal 2 hold a generation program of the same random data, To information which is included in an early response request message and/or a response message between the individual identification terminal 2 and the sized terminal 1 and which is enciphered. Include a value used as a seed value of the aforementioned random data, and henceforth in a message sent towards the individual identification terminal 2 from the sized terminal 1. Include random data made to generate this seed value as an initial value, and random data which made the aforementioned seed value an initial value by a generation program of the aforementioned random data also in the individual identification terminal 2 is computed, a case where comparative collation was carried out to random data contained in the aforementioned message sent towards the individual identification terminal 2 from the sized terminal 1, and both random data is in agreement -- the individual identification terminal 2 -- the person himself/herself -- an identification system use method of either of claims 7-12 which carries out a reaction at the time of discernment affirmation given in a claim.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1]** the sized terminal 1 which has the infrared-ray-communication mechanism a which sends personal identification information -- and, ** An individual identification system which identifies an individual in this individual identification terminal 2 according to the contents of the aforementioned personal information including the individual identification terminal 2 which has the infrared-ray-communication mechanism b which can exchange the information about personal identification information through the infrared-ray-communication mechanism a as an element.
[Claim 2]Make personal identification information send from the infrared-ray-communication mechanism a, and the infrared-ray-communication mechanism b receives this personal identification information, and a case where this personal identification information is considered as conformity by collation in the individual identification terminal 2 -- the individual identification terminal 2 -- the person himself/herself -- an identification system use method according to claim 1 of identifying an individual by carrying out a reaction at the time of discernment affirmation.
[Claim 3]Dispatch of personal identification information in the infrared-ray-communication mechanism a is intermittent dispatch, and when this personal identification information sent intermittently is made incongruent by collation in the ** individual identification terminal 2, and/or, a time of it having become impossible for the ** individual identification terminal 2 to receive this personal identification information sent intermittently -- the individual identification terminal 2 -- the person himself/herself -- an identification system use method according to claim 2 of identifying an individual by carrying out a reaction at the time of discernment denial.
[Claim 4]An identification system use method according to claim 2 or 3 of random data being contained in personal identification information, including collation of this random data in an individual discernment act, and identifying an individual.
[Claim 5]An identification system use method according to claim 4 that random data is one sort or two sorts or more of random data chosen from a group which consists of pseudorandom numbers obtained by an output value and a pseudorandom-numbers generation program of a one-time password and a one-way hash function.
[Claim 6]An identification system use method of either of claims 2-5 which information enciphered by personal identification information is included, compares this information enciphered, and identifies an individual given in a claim.
[Claim 7]When a response request message is made to send from the infrared-ray-communication mechanism b and the infrared-ray-communication mechanism a receives this response request message, a case where made a response message transmit towards the individual identification terminal 2, and this response message is considered as conformity in the individual identification terminal 2 from the sized terminal 1 -- the individual identification terminal 2 -- the person himself/herself -- an identification system use method according to claim 1 of identifying an individual by carrying out a reaction at the time of discernment affirmation.
[Claim 8]Only when the individual identification terminal 2 is identifying an individual, to this

individual identification terminal 2. A specific response request message is made to send to the sized terminal 1 of a discrimination object, This sends a response message for the sized terminal 1 only to a specific response request message from this individual identification terminal 2, When the individual identification terminal 2 is changed into a state which can respond only to a response message from this sized terminal 1 and the individual identification terminal 2 furthermore is not identifying an individual,An identification system use method according to claim 7 which makes a response request message to the unspecified sized terminal 1 send to the individual identification terminal 2, and changes the sized terminal 1 into a state which can respond only to a this object unspecified response request message.

[Claim 9]An identification system use method according to claim 7 or 8 of random data being contained in a response request message and/or a response message, including collation of this random data in an individual discernment act, and identifying an individual.

[Claim 10]An identification system use method according to claim 9 that random data is one sort or two sorts or more of random data chosen from a group which consists of pseudorandom numbers obtained by an output value and a pseudorandom-numbers generation program of a one-time password and a one-way hash function.

[Claim 11]An identification system use method of either of claim 9 or 10 which information enciphered by a response request message and/or response message is included, compares this information enciphered, and identifies an individual given in a claim.

[Claim 12]** Dispatch of a response request message is intermittent dispatch, and/when a response message which receives that it can come was made incongruent in the individual identification terminal 2. or ** -- a time of it having become impossible for the individual identification terminal 2 to receive a response message over this -- the individual identification terminal 2 -- the person himself/herself -- an identification system use method of either of claims 7-11 which identifies an individual by carrying out a reaction at the time of discernment denial given in a claim.

[Claim 13]Information which is different for every response request message in a part of response request message intermittently sent from the individual identification terminal 2 is included, To and a response message sent from the sized terminal 1 to each response request message. the aforementioned information -- or the double sign of the enciphered aforementioned information being carried out, and, when information which enciphered information which processed this information is included and the individual identification terminal 2 receives this response message, case it carries out comparative collation to this double sign information and information included in the aforementioned response request message and both information is substantially the same -- the individual identification terminal 2 -- the person himself/herself -- an identification system use method of either of claims 7-11 which performs a reaction at the time of discernment affirmation given in a claim.

[Claim 14]The sized terminal 1 and the individual identification terminal 2 hold a generation program of the same random data, To information which is included in an early response request message and/or a response message between the individual identification terminal 2 and the sized terminal 1 and which is enciphered. Include a value used as a seed value of the aforementioned random data, and henceforth in a message sent towards the individual identification terminal 2 from the sized terminal 1. Include random data made to generate this seed value as an initial value, and random data which made the aforementioned seed value an initial value by a generation program of the aforementioned random data also in the individual identification terminal 2 is computed, a case where comparative collation was carried out to random data contained in the aforementioned message sent towards the individual identification terminal 2 from the sized terminal 1, and both random data is in agreement -- the individual identification terminal 2 -- the person himself/herself -- an identification system use method of either of claims 7-12 which carries out a reaction at the time of discernment affirmation given in a claim.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]This invention is an invention about the system and directions for use for identifying an individual in an electronic terminal. This invention is still more specifically an invention about said system which used the infrared ray communication function, and its directions for use.
[0002]
[Description of the Prior Art]Conventionally, identification with a password is used most widely as an individual identification device in an electronic terminal. Generally this technique The keyboard of a computer to that individual's ID information. (For example, a staff number) and passwords (password etc.) are entered, those who will operate it if they are in agreement with what is registered into the computer a priori admit being the person himself/herself, and subsequent operation is permitted.
[0003]Next, register ID information, a password, etc. into the magnetic card or the IC card, this is made to read with the card reader connected to the computer, and the method of identifying an individual, the method which combined this and the above-mentioned keyboard input, etc. are mentioned. It also became possible to reduce the time and effort which improves safety and inputs ID information etc. from a keyboard by these so that it cannot be operated, if it is not human being with a card for example, even if a password etc. are revealed to others.
[0004]The art which identifies a fingerprint these days or carries out identification by what is called biological information [say / the pattern of the iris of eyes, a voiceprint, etc.] is being developed. Although there is a danger of it being stolen or being forged, in case of a card, if it is biological information, in this point, it is safe.
[0005]However, a problem which each mentions later is observed in these methods.
[0006]
[A technical problem for an invention to be solved] One and a decisive problem are observed in the conventional individual identifying method. It is that it is required at the time of discernment for a discrimination object person to do a certain operation being conscious of it. That is, before starting operation of an electronic terminal, it must change into the state where operation cannot be resumed unless it enters a password from a keyboard, it carries out end processing at the time of a leaving chair so that it may not be used for others after that, and it enters a password again. It is also the same as when using a card, a card must be inserted in a reader before an operation start, and a card must be sampled and carried at the time of a leaving chair. Also in biological information, it must operate pressing a finger against a fingerprint reader several seconds etc. before operation, for example.
[0007]The same state continues for a long time, if identification is completed, if these individual identifying methods are cases so that a leaving chair may not be carried out for having robbed for a discrimination object person, it can once be equal [individual identifying methods] to use but somehow, and carrying out a leaving chair frequently depending on the character of a discrimination object person's business is also assumed. When such a leaving chair is frequent, whenever it takes a seat, same identification operation must be performed. In such a case, since

human being dislikes troublesome work fundamentally, end processing will be just neglected, or a seat will be left, with a card inserted, and the possibility of the accident in which data tries to be stolen by others in a leaving chair, or it is altered will become very high. However it may introduce an expensive and advanced discrimination system, when employment that a card is inserted is made, the security function of identification will completely become meaningless.
[0008]Therefore, if the work of this identification can be performed without carrying out operation special to an operator, Before a discrimination object person is conscious at all, it is ideal that a system carries out automatically and it becomes possible by realizing this to secure the safety of the identification whole system also including an aspect of practical use.
[0009]Although it examined whether a noncontact IC card could be used for such a use, such an IC card is structure which communicates by electromagnetic waves via the small coil embedded on the card.
Transceiving equipment will become at an expensive price and large-sized.
Therefore, although the noncontact IC card is suitable for use in the ticket gate of a station, the tollgate of a highway, etc., installing in all the computer terminals in an office has unreasonableness, for example. Directive control and cover are difficult for electromagnetic waves, and it is difficult to classify each communications area clearly. Therefore, in the operational environment of a computer terminal being densely arranged like [in an office], and also moving frequently by the spread of notebook PCs, it is very difficult to communicate without interfering in a computer terminal group mutually.
[0010]
[Means for Solving the Problem]this invention person thought out by using infrared ray communication for an individual identification system wholeheartedly as a result of examination for the above-mentioned technical problem to be solved.
[0011]Infrared ray communication is one of the art which has spread widely with the remote control of television or video, and is most widely used for indoor short distance communication. The latest notebook sized personal computer is almost equipped with an infrared ray communication unit as standard, and that by which a small computer called a Personal Digital Assistant and a handheld game machine which go into a pocket is also equipped with an infrared ray communication unit has spread widely. A device and software for exchanging information by infrared ray communication also spread, and, as for standard agreement of information exchange, IrDA etc. are partly enacted for these portable computers, a common computer, or a network. Therefore, suitable software for the existing general-purpose art is only used for making automatic identification possible by infrared ray communication, and it means solving a technical problem about identification mentioned above.
[0012]Since infrared rays are a kind of light, they are easy to control grasp of an infrared ray communication unit. That is, fundamentally, a light-receiving-and-light-emitting device part of an infrared ray communication unit is a range (from several centimeters to about several meters) which looks mutual, and the grasp of an infrared ray communication unit can cover even one sheet of paper simply. Easy and grasp setting out with cheaply high flexibility can be performed also by using common optical tools, such as a lens and a mirror.
[0013]the sized terminal 1 in which this invention person specifically has the infrared-ray-communication mechanism a which sends ** personal identification information in this application -- and, ** In [including as an element the individual identification terminal 2 which has the infrared-ray-communication mechanism b which can exchange the information about personal identification information through the infrared-ray-communication mechanism a] this individual identification terminal 2, the various directions (: hereafter called this system-usage method -- it still more specifically mentions later) for an individual identification system (henceforth this discrimination system) which identifies an individual according to the contents of the aforementioned personal information, and this system are provided.
[0014]
[Embodiment of the Invention]Hereafter, the contents of this invention are explained, using a drawing. Drawing 1 is a drawing (front view) in which the outline of this recognition system is shown.

[0015]The infrared light-receiving-and-light-emitting device 11 in which this recognition system 100 displayed on Drawing 1 is the infrared-ray-communication mechanism b of ** above is connected, . The software which processes the electronic intelligence from this infrared light-receiving-and-light-emitting device 11, and identifies an individual at least was incorporated. The computer 10 which works as the above-mentioned individual identification terminal 2, and the small computer 20 (in Drawing 1) which works as the above-mentioned sized terminal 1 in which the infrared light-receiving-and-light-emitting device 21 which is the infrared-ray-communication mechanism a of ** above was incorporated the small computer 20 is carried by the discrimination object person 30 -- **** -- it is constituted.
[0016]In using this recognition system 100, are in the state in which communication according [the infrared light-receiving-and-light-emitting device 11] to infrared rays is possible at least, and the discrimination object person 30, The small computer 20 is carried and the infrared light-receiving-and-light-emitting device 21 formed in this is also in the state in which communication by infrared rays is possible as a principle.
[0017]Here, if it is an electronic terminal which recognizes an individual and operates him as a kind of the above-mentioned individual identification terminal 2, it is not limited in particular and network terminals including a computer as shown in Drawing 1, the security additional equipment, etc. can be illustrated.
[0018]Here, the security additional equipment is a device which adds the function of this invention to other devices. For example, by computer traditional type, when the infrared-ray-communication mechanism b is not connectable with this, or also when software required for an individual's discernment cannot be mounted, it thinks. In such a case, that to which this computer connected the controllable switching and balancing box can be used for the small computer which mounted the minimum function required for an individual's discernment as security additional equipment. In the security additional equipment illustrated here, connecting a keyboard and a display with a computer body traditional type [above] via a switching and balancing box can give the outstanding safety by this recognition system to this computer. Namely, at the time of identification affirmation the security additional equipment, The switch of the switching and balancing box can be changed into the state of ON, and it can carry out as [be / the display of the operation or the display by a keyboard / possible], and said switch can be changed into the state of OFF at the time of identification denial, and the operation and the display by a keyboard can be indicated impossible. In this case, although the end etc. of the business program which is moving by the computer traditional type [aforementioned] are uncontrollable, since reservation of security sufficient by just controlling operation and a display can be performed in many cases, it is useful enough. The applicable field of this recognition system is expandable by connecting with the closing mechanism of a door metallurgy warehouse, or connecting such security additional equipment to machinery, a device, etc. with which only authorized personnel were allowed operation, for example.
[0019]If it is an electronic terminal as a kind of sized terminal 1 which can usually be carried around by the individual, especially, it is not limited and a small computer, a handheld game machine, a Personal Digital Assistant, a portable telephone terminal, etc. as shown in Drawing 1 can be illustrated, for example.
[0020]the infrared light-receiving-and-light-emitting device 11 -- said -- if the communication available area of 21 is set up as shown in Drawing 2 (top view) (the communication available area of the infrared light-receiving-and-light-emitting device 11 in the slash field A) [show and] said, when i discrimination object person 30 does not operate the computer 10 but is separated from the computer install stand 40, for example, the slash field B shows the communication available area of 21, communication-available-area A-B does not overlap mutually -- the infrared light-receiving-and-light-emitting device 11 -- said -- since 21 cannot be communicated, the computer 10 detects a discrimination object person's absence, and processing required for security reservation, such as a lock of a keyboard, elimination of the contents of a screen display, and end processing, is made automatically. ii when the discrimination object person 30 operates the computer 10, the infrared light-receiving-and-light-emitting device 11 -- said -- 21, since it confronts each other so that mutual communication feasible region A-B may overlap,

the infrared light-receiving-and-light-emitting device 11 -- said -- communication of the computer 10 and the small computer 20 is attained via 21, and the information for the identification which the discrimination object person 30 holds in the small computer 20 is received in the infrared light-receiving-and-light-emitting device 11. And the computer 10 performs identification processing automatically based on this personal identification information, and after recognizing the discrimination object person 30, 10 can be automatically made into an operable state. In this recognition system 100, the above-mentioned illustration states i and ii can be automatically changed by the discrimination object person's 30 action.

[0021]Thus, in this discrimination system 100, The small computer 20 into which the discrimination object person 30 inputted own right personal identification information is only carried, the discrimination object person 30 person himself/herself does not even do special operation or consciousness, and security reservation of the system for which it asks by suitable identification is automatically possible.

[0022]In infrared ray communication, by adjusting the intensity of an infrared beam, and the width of a beam, it is possible to control grasp simply and it can cover still more easily.

[0023]Drawing 3 is a schematic diagram (top view) of this recognition system in the case of being crowded with the above-mentioned individual identification terminals 2. Three sets of the above-mentioned individual identification terminals 2 to which the above infrared light-receiving-and-light-emitting device b is connected respectively are shown on computer install stand 40' by Drawing 3. [The computer 10A (the infrared light-receiving-and-light-emitting device 11A is connected), said 10B (the infrared light-receiving-and-light-emitting device 11B is connected), said 10C (the infrared light-receiving-and-light-emitting device 11C is connected)] .The small partition (61A, 61B, 61C) which can cover infrared rays is installed in order to cover dispersion to left-hand side near each infrared light-receiving-and-light-emitting device b toward the computer of the infrared rays sent from each infrared light-receiving-and-light-emitting device b. The large partition (62A, 62B, 62C) which can cover infrared rays is installed in the direction of this side of computer install stand 40' in order to cover dispersion to right-hand side toward the computer of the infrared rays sent from each infrared light-receiving-and-light-emitting device b.

[0024]It is possible to install a partition, as shown in Drawing 3, and to adjust the communication feasible region by infrared rays suitably like the communication feasible region C, D, and E, for example. Namely, as shown in this figure, even if it is a case as the computer 10 crowds and is arranged, It is possible to identify two or more recognition object persons in each individual identification terminal easily, without arranging the communication feasible region by infrared rays, and interfering mutually by forming the barrier to infrared rays, such as a partition.

[0025]Generally, since the communication feasible region by infrared rays is about at most several meters, it is so clearer than the case where the electromagnetic waves and network communication of a wide area are used that its the degree of safe of this recognition system is excellent that a communication feasible region is not compared.

[0026]the thing of a form simple as a mode of use of this recognition system, for example, (1), -- intermittently an individual ID number and a password by infrared ray communication as a message of a plaintext with a suitable time interval. [then,] It transmits towards the individual identification terminal 2 from the sized terminal 1, and the individual identification terminal 2 checks receiving contents. And if these receiving contents are in agreement with the individual ID number and password which are registered into the terminal 2, they will identify that he is a discrimination object person, and to the following individual ID number and reception of a password, the individual identification terminal 2 -- the person himself/herself -- it is also possible to use this recognition system which repeats the process in which it reacts at the time of discernment affirmation.

[0027]Namely, this invention makes personal identification information send from the infrared-ray-communication mechanism a, the case where the infrared-ray-communication mechanism b received this personal identification information, and this personal identification information is considered as conformity by the collation in the individual identification terminal 2 -- the individual identification terminal 2 -- the person himself/herself -- it is the invention which

identifies an individual and which provides the directions for this discrimination system by carrying out the reaction at the time of discernment affirmation.
[0028]However, this system-usage method of this is hard to be called safety perfectly in the case where a third party with the bad faith of monitoring a communication content intervenes etc. For example, as shown in Drawing 4 (top view: especially a sign applies to Drawing 2 unless it refuses), Near the infrared light-receiving-and-light-emitting device 11, the above malicious third parties 70 install the infrared light-receiving device 71 secretly, and the contents of the infrared ray communication by the just discrimination object person 30 with the reader 72. The case where it monitored and records is assumed (80 shall express among a figure the means which makes it possible to conceal interception / record action by the third party 70 from the discrimination object person 30 etc., for example, a barrier etc.). With in this case, the infrared ray communication unit which the third party 70 owns after the discrimination object person 30 does a leaving chair. If it precedes, and interception, and the discrimination object person's 30 ID number and password which were recorded are turned to the infrared light-receiving-and-light-emitting device 11 and sent, the third party 70 will become possible [operating spoofing and the computer 10 unjustly to the discrimination object person 30].
[0029]Therefore, in the system treating the information that confidentiality and importance are high, the device by such interception and tapping which cannot become completely and ** is needed. As such an example, for example the individual identification terminal 2 of (2) above, Data in which the same value does not appear intermittently in a suitable time interval repeatedly (in this invention) Information including the pseudo-random number and one-time password of sufficient digit number to prevent the same value from repeating accidentally for example, such data is also called random data, the output value of a one-way hash function mentioned later, etc., The sized terminal 1 which transmitted towards the above-mentioned sized terminal 1, and received this enciphers this information with the secret key which a discrimination object person holds, for example, turns this encipherment information to the individual identification terminal 2 with a discrimination object person's ID number, and transmits. And if the individual identification terminal 2 finds out the public key which corresponds this transmit information from said ID number, transmit information is decoded, the first origination information that this decoded data and individual identification terminal 2 have memorized is compared and both are in agreement, It is possible to identify that a discrimination object person is genuine.
[0030]In [if this processing is repeated intermittently and performed, the information on different contents one after another from last time will be transmitted for every constant interval towards the sized terminal 1 from the individual identification terminal 2, and] the sized terminal 1, Information different each time [these] will be enciphered one after another with a self secret key, and it will transmit towards the individual identification terminal 2. Therefore, since this third party does not grasp about the secret key in the sized terminal 1 even if the holder in bad faith who tries interception and record of this communication content monitors, It is impossible to be unable to encipher correctly the information transmitted one after another from an individual identification terminal, but to become a genuine discrimination object person, and to clear up.
[0031]Namely, the pseudorandom numbers in which this invention is obtained by a one-time password and the pseudorandom-numbers generation program at personal identification information, The directions for this discrimination system which the random data of the one-way hash function etc. which are mentioned later is contained, includes collation of this random data in an individual discernment act, and identifies an individual, And it is also the invention which provides the directions for this discrimination system which the information enciphered by personal identification information is included, compares this information enciphered, and identifies an individual.
[0032]Also in this system-usage method using the random data enciphered, for example, The above malicious third parties are considered for it to be also possible theoretically for to become a genuine discrimination object person and to clear up, if interception of information can be continued over a long time and the group of transmit information can all be recorded. However,

by enlarging random nature of random data enough, By for example, the thing (for example, about 10 or more figures) for which the digit number of the pseudorandom numbers used as random data is set up greatly enough. It can also be made to take huge time to monitor and record information, and the thing which is moreover a third party in making a change of a secret key etc. suitably and which it receives clearing up and is opposed nearly perfectly as soon as it is malicious is possible.
[0033]Although this method of (2) is improving safety using bidirectional communication and encoding technology, it is using a one-time password especially as random data, and one-way communication can also secure comparable safety. If this is made into an example (3), the individual identification terminal 2 and the sized terminal 1 will both hold (3) discrimination-object person's secret password, and both these terminals 1 and 2 of both will assume that the fitness clock register is held. And in the sized terminal 1, vacate a suitable interval, and the secret password of the time information in the time and a discrimination object person is combined intermittently, A hash value is calculated by inputting this connected information into a one-way hash function, it is made to go via infrared light-receiving-and-light-emitting device b-a, and the information which added ID information etc., the calculation result, i.e., one-time password, is transmitted to the individual identification terminal 2. And the individual identification terminal 2 which received this information, Combine the password which searched the discrimination object person's [/ based on the ID information to hold] secret password, searched with the time information in the time, and became clear, and it inputs into the same function as the above-mentioned one-way hash function, If a hash value is computed, the hash value obtained again is compared with the hash value already transmitted from the sized terminal 1 and these hash values are in agreement, it is possible to check that he is a genuine discrimination object person.

[0034]Although time information is used twice and both time information needs to be in agreement in this example (3), since the error of the clock registers which the individual identification terminal 2 and the sized terminal 1 hold, few time lags of hour corresponding, etc. are accepted, it is necessary to define appropriately setting out and the permissible error of the unit of time information. For example, when the unit of time information is carried out to to a second and a permissible error is made into less than [plus-or-minus 1 second], When the hash value obtained in the individual identification terminal 2 is as inharmonious as the hash value obtained with the sized terminal 1, the value for "time **1 second added with the individual identification terminal 2" is used and re-calculated, and when a hash value is inharmonious, and a discrimination object person is an un-genuine person, it will still come to a conclusion.
[0035]Although some kinds, such as CRC, MD4, MD5, Snefu, SHA-1, and a checksum function, are observed in a one-way hash function, Even if it uses which function, calculation is easy compared with an unsymmetrical key code etc., there is also little processing time, it ends, and the input data of a basis cannot be computed from a hash value, but the feature that it is very difficult to find different input data with the same hash value is accepted.
[0036]Thus, this invention is an invention which provides the identification system use method described in the above (1) that the one-time password is contained in personal identification information.
[0037]Although there are few methods (3) of using this one-time password, and they end and computational complexity and their traffic are efficient compared with the method of (2), the time information in the individual identification terminal 2 and the sized terminal 1 must be less than a fixed error, and the problem that matching the time must be carried out periodically is also accepted. The following method as shown in (4) is also considered as an efficient method without such a problem.
[0038](4) Make the individual identification terminal 2 and the sized terminal 1 completely hold the generation program of the random data of the same pseudorandom-numbers generation program etc., and exchange of the first information in both terminals, An unsymmetrical key code etc. perform and, simultaneously with the check of being the right sized terminal 1, the initial value (seed value) given to the generation program of random data is also included in the enciphered information which is sent to the sized terminal 1 from the individual identification

terminal 2. Henceforth, with a suitable time interval, the sized terminal 1 generates the random data R (R1, R2, R3, ...) one after another based on this seed value, is in the state (division into equal parts) which does not encipher ID information and the information containing random data, and transmits to the individual identification terminal 2. Next, the individual identification terminal 2 also calculates the random data r (r1, r2, r3, ...) by giving the same seed value to the same random data generation program. Since the generation program and seed value of random data of both terminal b-a are the same as mentioned above, right R by which backward transfer is carried out from the sized terminal 1 will certainly be in agreement with r. That is, when this identity of R and r is maintained, it can check that a discrimination object person is genuine.

[0039]Namely, this invention holds the generation program of random data with same sized terminal 1 and individual identification terminal 2, To the information which is included in the early response request message and/or response message between the individual identification terminal 2 and the sized terminal 1 and which is enciphered. Include the value used as the seed value of the aforementioned random data, and henceforth in the message sent towards the individual identification terminal 2 from the sized terminal 1. Include the random data made to generate this seed value as an initial value, and the random data which made the aforementioned seed value the initial value by the generation program of the aforementioned random data also in the individual identification terminal 2 is computed, the case where comparative collation was carried out to the random data contained in the aforementioned message sent towards the individual identification terminal 2 from the sized terminal 1, and both random data is in agreement -- the individual identification terminal 2 -- the person himself/herself -- it is the invention which carries out the reaction at the time of discernment affirmation and which provides the directions for this discrimination system.

[0040]In this case, though the malicious third party of interception and record of information has monitored communication of both terminal b-a, since the seed value itself is enciphered, this third party cannot know those true contents, and the above-mentioned random data R cannot be computed. That is, the above-mentioned holder in bad faith turns into a genuine recognition object person, and can clear up.

[0041]In this method (4), when communication is interrupted once, it will resume from exchange of the enciphered seed value. The individual identification terminal 2 made it generate by the generation program of random data, etc. uniquely each time, and the seed value exchanged, of course must be made into the value which an external thing cannot predict at all.

[0042]In this method (4), only the initial stage of a discernment process is required for two-way communication, And although an operation process must be [which it was called encryption and decryption] comparatively complicated and it must pass through the process where a burden is placed on an electronic terminal, unless communication is interrupted henceforth, It is one-way communication and the safety for which it asks can be secured only by the calculation for moreover computing the random data of a simple pseudo-random number etc.

[0043]Infrared ray communication has the feature which is easy to manage a communications area compared with the case where electromagnetic waves etc. are used as mentioned above. However, to a certain individual recognition terminal 2, a one discrimination object person is already in a communication feasible region, and a possibility by the sized terminal 1 which this recognition object person holds that other discrimination object persons will go into this communication feasible region in the midst of identification still cannot be denied, either. Therefore, it is desirable to lecture on a means by which a discernment process is made to be performed correctly, even if it is such a case.

[0044]As such a means, the method (5) described below can be illustrated, for example. (5) When the individual identification terminal 2 is the object waiting of identification when nobody's discrimination object person is in the communication feasible region of the individual identification terminal 2 namely, this individual identification terminal transmits preferably the response request message G1 to an unspecified person intermittently with a suitable time interval. The sized terminal 1 which the discrimination object person who received this holds will disregard this response request message G1, if it is communicating with other individual identification terminals 2, and if it is not [be / it] under communication, it will transmit response

message F1 over this G1 to the individual identification terminal 2 which is sending the response request message G1. Since the discrimination object person's ID information which the sized terminal 1 holds is included in this response message F1, the individual identification terminal 2 transmits henceforth the response request message G2 only by turning to the sized terminal 1 which has transmitted that F1. Since the discrimination object person's ID information is included in this response request message G2, the sized terminal 1 which received this, The ID information included in these G2 is checked, and only when it becomes clear that this message G2 is turned to self, suppose that the response message F2 over it is transmitted to the individual identification terminal 2.

[0045]While identification of someone has already been carried out in a certain individual identification terminal 2 by doing in this way, even if discrimination object someone else (the sized terminal 1 is held) approaches, it is possible to prevent malfunction of this system by mutual interference etc.

[0046]Thus, this invention makes a response request message send from the infrared-ray-communication mechanism b, When the infrared-ray-communication mechanism a receives this response request message, a response message is made to transmit towards the individual identification terminal 2 from the sized terminal 1, Only when this response message is considered as conformity in the individual identification terminal 2, the individual identification terminal 2 -- the person himself/herself -- the directions for this discrimination system which identifies an individual being provided, and further by carrying out the reaction at the time of discernment affirmation, Only when the individual identification terminal 2 is identifying the individual, to this individual identification terminal 2. A specific response request message is made to send to the sized terminal 1 of a discrimination object, This sends a response message for the sized terminal 1 only to the specific response request message from this individual identification terminal 2, When the individual identification terminal 2 is changed into the state which can respond only to the response message from this sized terminal 1 and the individual identification terminal 2 furthermore is not identifying the individual, It is the invention which makes the response request message to the unspecified sized terminal 1 send to the individual identification terminal 2, and changes the sized terminal 1 into the state which can respond only to a this object unspecified response request message and which provides the directions for this above-mentioned discrimination system.

[0047]To the response request message and/or response message of ** above. random data (the pseudorandom numbers obtained by a one-time password and the pseudorandom-numbers generation program.) It is preferred for the output value of a one-way hash function, etc. to be included, and to include collation of this random data in an individual discernment act, It is preferred for the information enciphered by ** response request message and/or the response message to be included, to compare this information enciphered, and to identify an individual, and further, i Dispatch of a response request message is intermittent dispatch, and **/when the response message which receives that it can come was made incongruent in the individual identification terminal 2. or ii -- the time of it having become impossible for the individual identification terminal 2 to receive the response message over this -- the individual identification terminal 2 -- the person himself/herself -- it is preferred by carrying out the reaction at the time of discernment denial to identify an individual.

[0048]And information which is different for every response request message in a part of response request message where this invention is intermittently sent from the individual identification terminal 2 in this desirable mode is included, To and the response message sent from the sized terminal 1 to each response request message. the aforementioned information -- or the double sign of the enciphered aforementioned information being carried out, and, when the information which enciphered the information which processed this information is included and the individual identification terminal 2 receives this response message, case it carries out comparative collation to this double sign information and the information included in the aforementioned response request message and both information is substantially the same -- the individual identification terminal 2 -- the person himself/herself -- it is the invention which performs the reaction at the time of discernment affirmation and which provides the directions

for this above-mentioned discrimination system.
[0049]When the state 2 which is in the communication feasible region of the individual identification terminal 2, i.e., an individual identification terminal, is in the state of the waiting for discernment, this individual identification terminal 2 is an always suitable time interval, and the response request message to an unspecified person will continue being transmitted intermittently, but. Generally, as the individual identification terminal 2 was already described using the drawing, it is the electronic terminal installed in desk superiors in many cases, and AC power supply is supplied in many cases, and the continuous transmission of a message does not pose a problem in particular. On the other hand, it is a portable electronic terminal, and since the sized terminal 1 has a limit in the capacity of a battery, it is preferred [the sized terminal / the transmission amount of the infrared rays which consume power] to press down as much as possible. In the example of (5) mentioned above, it is only a time of receiving the response request messages G1 and G2 that the sized terminal 1 transmits infrared rays towards the individual identification terminal 2. In the case in the state where it does not identify, a discrimination object person also in which individual identification terminal specifically, For example, when the discrimination object person who holds the sized terminal 1 is holding a meal, a meeting, etc. and does not do the work interlocked with the individual identification terminal 2 for a long time. The sized terminal 1 is in the state of the waiting for reception about the response request message for the unspecified persons from the arbitrary individual identification terminals 2, and infrared transmission is not performed. For this reason, this means of (5) is effective also in the meaning which extends the battery temporal duration of the sized terminal 1.
[0050]Kerberos etc. which are becoming a standard can be used as a network authentication protocol as information which the sized terminal 1 and the individual identification terminal 2 other than an example which have so far been described exchange for identification.
[0051]This discrimination system is dramatically useful as an individual identification system in the electronic information system which recognizes a specific individual and works. The electronic information system which is the use target of this discrimination system, Although not limited at all, confidentiality is high especially, and moreover, the user of an electronic information system is busy and it is suitable to use for the system by which turning on and off this system frequently is assumed, for example, an electronic chart, a banking system, a security system, a military system, etc.
[0052]
[Example]Hereafter, this invention is explained still more concretely using an example. However, this example should not carry out the limited interpretation of the technical scope of this invention. Although it is as having mentioned above, in this example, it explains that this invention is useful on all the aspects of affairs that need identification taking the case of the medical system treating an electronic chart etc. which is one of the systems which need the severest security management.
[0053]A medical system is a system treating the important information to affect people's life. A patient's privacy protection, a name of a disease notice problem, etc. are a system which especially the security of information takes cautions.
However, the medical practitioner and nurse handling this system are dramatically busy, for example, it is an everyday occurrence for a medical practitioner to hurry medical examination information and to do a leaving chair to an electronic chart system moreover during an input, for several hours for an emergency case, change of hospitalization condition, etc. Therefore, in such a system, even if it performs identification and attestation by the conventional IC card etc., While the medical practitioner had been inserted [the IC card] carelessly, after separating from a system terminal, it will be neglected while the system has been in the state of ON, and anyone can operate a system freely, and it has been a big problem on security.
[0054]This example is the embodiment which took the example in the importance of this discrimination system in such a medical site. In Drawing 2 mentioned above, the small portable computer 20 which has an infrared ray communication function is distributed to discrimination object person 30 all the members (plurality : specifically as a principle a medical practitioner, a

nurse, an inspecting engineer, etc.) in this discrimination system 100. The administrator (not shown) of a system assigns the pair (public key P-key and secret key S-key) of the key of an unsymmetrical key code to discrimination object person 30 all the members a lot every, and to the portable computer 20. Before the discrimination object person's 30 distribution, these candidates' ID (staff number etc.) and S-key are registered.

[0055]The contents of S-key of the portable computer 20 can be seen, or it prevents from having changed except the system administrator. Discrimination object person 30 all the members' ID and the conversion table of P-key are registered into the computer 10 of the medical system, and it enables it to refer to P-key of the personnel with specific ID in the computer 10.

[0056]The key point in the hospital where this discrimination system 100 is used for the computer 10. Two or more sets are suitably installed in (for example, a consultation room, an operating room, a laboratory, a nurse's station, an office, etc.) (as for each computer 10, it is preferred to have the function which can exchange information electronically). Individual ID (terminal number etc.) is inputted into each computer 10. The infrared light-receiving-and-light-emitting device 11 is connected to all the computers 10 directly or indirectly.

[0057]In the state of the waiting for discernment, the computer 10 response request message G1:G1:A0011 to an unspecified person (when ID of the computer 10 is "A0011"), It continues (by shortening a time interval, a reaction when the attestation candidate 30 approaches the computer 10 can be carried out early) transmitting with infrared rays with a short time interval, for example, a 0.1-second interval grade.

[0058]For example, the one computer 10 is installed in the consultation room. The medical practitioner 30 who is a discrimination object person attaches to the breast the right portable computer 20 with which their ID information and S-key were registered. Although the infrared light-receiving-and-light-emitting device 21 is connected also to the portable computer 20, it is a reception waiting state which does not transmit at all from some computers 10 until it receives the response request message G1.

[0059]The medical practitioner 30 goes into a consultation room, the computer 10 is approached, and it is the physical relationship with which the infrared light-receiving-and-light-emitting devices 11 and 21 can communicate. When it becomes [Drawing 2 (2)], the portable computer 20, The response request message G1 is received from the computer 10 via the infrared light-receiving-and-light-emitting devices 11 and 21, Response message F1:F1:D0135:A0011 is immediately transmitted towards the computer 10 via the infrared light-receiving-and-light-emitting devices 21 and 11 (when the medical practitioner's 30 ID is "D0135"). Since the medical practitioner's 30 ID information is included in response message F1, in the computer 10. Search each recognition object person's ID registered, and P-key corresponding to the medical practitioner's 30 ID is found out, Message G2:G2:D0135:A0011:3eb%78xdc-92ef containing the message R enciphered by this P-key (by S= 7359224781.) The case where R which enciphered this is "3eb%78xdc-92ef" is transmitted to the portable computer 20. In this example, what enciphered the pseudorandom-numbers character string S which made it generate when the computer 10 received response message F1 is set to R.

[0060]By S-key registered into this, the portable computer 20 which received this message G2 decodes the message R contained in the message G2, and obtains the character string S. Since only the portable computer 20 with secret key S-key can decode the message R correctly, it is this stage and 10 and 20 will share correctly the secret information S which is not known by the others. The portable computer 20 receives the message G2 correctly, in order that it may tell the computer 10 about preparation having been completed, turns response message F2:F2:D0135:A0011 to the computer 10, and transmits.

[0061]The computer 10 which received the response message F2 transmits response request message G3:G3:D0135:A0011:163 to the portable computer 30 intermittently henceforth (when SEQ is "163"). Although the field called SEQ is included in response request message G3, this is a sequence number which shows a number of G3 that the computer 10 transmits it is, and is a kind of counter.

[0062]The portable computer 20 which received response request message G3, The value H

which can compute only the computer 10 and the portable computer 20 based on the character string S of the shared secrecy mentioned above using MD5 which is a one-way hash function is computed, Response message F3:F3:D0135:A0011:163:9e3bcf73d48f99eca865465caf679e77 containing this H are transmitted to the computer 10. Even if a third party monitors said message G3 and F3 at this time, it will be preferred on security to prevent F3 which should be sent to the next from predicting for a third party. Although there is random data (this may be enciphered) mentioned above as this prediction impossible-izing means, even if it is un-random data, this can also be made prediction impossible with the output value processed by the one-way hash function (it mentioned above). If input data of a one-way hash function is completely the same, the same hash value will be computed as an output value, but the hash value which MD5 outputs, for example like the above-mentioned example is a numerical value as big as 128 bits (they are 32 figures by hexadecimal number display).
If input data is more nearly different, a completely different hash value will be outputted.
Input data cannot be drawn from a hash value, or it cannot predict.
[0063]In the response message F3, SEQ is the same value as SEQ contained in response request message G3 which received immediately before. After exchanging the contents of the character string S between the computer 10 and the portable computer 20, the value of SEQ of the first response request message G3 increases every [1] one by one with 2, 3, 4, and ... henceforth by one. Next, the value H is a hash value computed by inputting into one-way hash function MD5 the information acquired by combining the character strings S and SEQ. In this case, supposing it is the character string S= 7359224781, H of the response message F3 which transmits first will be calculated by MD5 (7359224781-1), and
"fc4d94633e5f4128959e3d6a77fde4eb" will be computed.
[0064]Similarly H of the response message F3 which transmits to the 2nd is calculated by MD5 (7359224781-2), and "5baab4f5876b1ee9869e0b02ceccbe8e" is computed.
[0065]Input data only changed one of SEQ which is an end to 2 so that it might understand also in this example, but the hash value is a completely different value, and when a deer next also changes SEQ to three, H is incalculable if right S is not known.
[0066]In this example, the response message F3 has become SEQ which described it as hash value H previously, and also discernment of the message from the medical practitioner's 30 ID number, and the ID number of the computer 10.
[0067]The computer 10 which received the response message F3 checks the ID number for discernment first, and it is a message addressed to itself.
And it checks that it is a thing from the medical practitioner 20 who is going to identify now.
The computer 10 checks that SEQ contained in the response message F3 is in agreement with SEQ of response request message G3 which self sent immediately before. After this coincidence is accepted, hash value h is computed by inputting into one-way hash function MD5 the secret value S which the SEQ and computer 10 self hold like the portable computer 20. If comparative collation of computed h and the H contained in the response message F3 is carried out and both hash value is in agreement, as for the computer 10, the medical practitioner 30 will allow the processing at the time of discernment affirmation, i.e., operation and a display of a system, as what was identified as an individual.
[0068]In this example, in order to maintain the security of a system, the computer 10 is the shortest possible time interval, should transmit response request message G3 one after another, and should check the response message F3 respectively returned to these. However, since the computer 10 and the portable computer 30 consume the calculation power and the battery of CPU for calculation or communication, In the suitable time interval according to employment of the security level and system which are demanded, and this example, it is preferred to set it as about 0.5 to 2 seconds.
[0069]Temporarily, since a possibility that a certain injustice is working is realized when inharmonious, in the computer 10, the hash values h and H will perform immediately the processing at the time of identification denial, i.e., the processing etc. for which elimination and the system operation of display information are made impossible. After response request message G3 transmission, even if predetermined time (for example, about 0.1 to 0.5 second)

passes, also when the computer 10 cannot receive the response message F3, processing at the time of the above-mentioned identification denial can also be performed immediately. However, since it thinks by the medical practitioner's 30 trifling operation etc. when communication is interrupted momentarily, response request message G3 can be resent and retry processing [say / waiting for the response message F3 again] can also be performed. Although the number of times, a time interval, etc. of this retry can set up a value suitable for employment, the time interval of retry time is [about 0.2 to 5 seconds] in general preferred about 2 to 10 times.
[0070]When identification is denied, an identification process will return to an initial state. That is, the computer 10 will cancel all of ID information, S, SEQ of the medical practitioner 30 who was identifying before this denial, etc., and will transmit the response request message G1 to an unspecified person again. On the other hand, if the portable computer 20 cannot carry out time (in general about 3 to 30 seconds) reception of predetermined, either, response request message G3 from the computer 10 which was being identified till then, S currently held till then, the ID information of the computer 10, etc. will be canceled, and it will return to the reception waiting state (initial state) of the response request message G1.
[0071]However, when identification is denied in this way, it is also possible to force the business program of the computer 10 to terminate, but. For example, even if it is such a case, the purpose can also be substantially attained by keeping a screen display and operation of a computer display from being possible during identification denial. For example, the same person performs an identification process from an initial state, and when identification is affirmed, it may enable it to resume a business program from a state just before identification is denied again, if it is in [from identification denial] fixed time. For example, the inspection during an input of a patient's medical record information with the easy medical practitioner 30 is needed, the leaving chair of this is carried out for 2 to 3 minutes, and a case so that he may like to resume the patient's medical record information inputting succeedingly is assumed.
[0072]Thus, in this example the communicative leadership, It is in the computer 10, and it is a waiting state, and the portable computer 20 side has usually taken the mode of turning the response message over this to the computer 10, and transmitting, only when a suitable response request message is received from the computer 10. In the case so that both the computer 10 by which the medical practitioner 30 is installed in the consultation room, and the computer 10 installed in an operating room may be used for this, for example. With the one portable computer 20 attached, whichever the medical practitioner 30 goes to ** only by adjusting appropriately an interval, retry time, etc. of dispatch time of response request message G3 according to the security level required of each **, he can receive suitable identification by it.
[0073]As mentioned above, the portable computer 20, In an initial state, receive only response request message G1 message for unspecified, and after this response request message G1 receptionist, Only the response request message G2 from the computer 10 which transmitted the G1 is received, after response request message G2 reception receives only response request message G3 from the computer 10 which sent out the G2, and other messages are disregarded.
[0074]Therefore, a certain computer 10 and computer 20 which the medical practitioner 30 carries in the state of identification, In the situation which is of continuing exchanging response request message G3 and the response message F3 mutually, Even if other persons, for example, a nurse, entered in that communication feasible region A-B, the portable computer which this nurse is carrying, Since response request message G3 transmitted from the computer 10 is disregarded and it does not react at all, The identification between the computer 10 and the portable computer 30 is not barred by interference etc., and personal authentication of this nurse is not necessarily conversely carried out accidentally in the computer 10.
[0075]
[Effect of the Invention]those who are going to operate electronic system by this invention -- infallible -- the person himself/herself -- a means by which the function which may be identified may be performed simple for an operator certain moreover by low cost is provided.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1]It is a drawing (front view) in which the outline of this recognition system is shown.
[Drawing 2]It is a drawing (top view) in which the outline of this recognition system is shown.
[Drawing 3]It is a schematic diagram (top view) of this recognition system in the case of being crowded with individual identification terminals.
[Drawing 4]It is a schematic diagram (top view) of this recognition system supposing a malicious third party's existence.

[Translation done.]